National Research Programme NRP 86 ‘Digital Resilience of Critical Infrastructures’

Call document

Table of contents

What are National Research Programmes (NRPs)?

Research carried out under National Research Programmes consists of research projects that contribute towards addressing societal challenges of national relevance.

Under the provisions of Article 10, paragraph 2, letter c of the Federal Act on the Promotion of Research and Innovation of 14 December 2012 (RIPA), the Federal Council selects the topics and focus areas to be researched in NRPs and mandates full responsibility for implementing the programmes to the Swiss National Science Foundation (SNSF). The Ordinance to the Federal Act on the Promotion of Research and Innovation of 29 November 2013 (RIPO), Articles 3-9, describes NRPs and their launch. According to this legal basis, two different processes can lead to the launch of an NRP:

1. Open rounds
2. Thematically defined rounds

The topic addressed in this NRP results from the second type of process and corresponds to current federal strategies and the priorities of the federal administration. In comparison to the open rounds process, this NRP aims at a shorter duration, a reduced budget, and a strengthened link between researchers and the federal administration. Scientific evaluation and funding decisions are carried out independently of political authorities and in accordance with the principles of scientific excellence and academic freedom.

On 1 July 2025, the State Secretariat for Education, Research and Innovation (SERI) mandated the SNSF to assess the feasibility of conducting an NRP on ‘Digital Resilience of Critical Infrastructures’ and to develop a programme concept that would define the aims and the key research issues to be addressed. Based on this programme concept, the Federal Council decided on 20 March 2026 to launch NRP 86 ‘Digital Resilience of Critical Infrastructures’. The members of its Steering Committee were elected by the National Research Council of the SNSF on 24 March 2026. The Steering Committee formulated this call for proposals and oversees the strategic management of the programme.

1 Summary

Proposals are invited for research projects to be conducted within the National Research Programme ‘Digital Resilience of Critical Infrastructures’ (NRP 86). The programme was mandated by the Swiss Federal Council on 20 March 2026 to strengthen the resilience of Switzerland's critical infrastructures against cyberattacks and other digital disruptions. It will fund research that improves the knowledge base on vulnerabilities and risks, develops technically viable and socially acceptable solutions, and proposes governance and coordination mechanisms for agile collective cyber defence. NRP 86 consists of four research areas:

- The ‘Data’ research area will examine what qualifies as relevant cybersecurity data and how access to, curation of, protection of and sharing of such data can be improved between academia, public authorities and critical infrastructure operators.

- The ‘Best practices’ research area will assess which organisational, technical and operational practices can be regarded as state of the art and how they can be adopted, tested, adapted and transferred across Swiss critical infrastructure sectors.

- The ‘Incentives’ research area will investigate the economic, regulatory, behavioural and institutional conditions that shape cybersecurity investment and identify ways to align organisational decisions with system-level resilience.

- The ‘Collective defence’ research area will explore how operators, suppliers, authorities, regulators, researchers and users can coordinate responsibilities, information exchange, risk assessment and joint responses before, during and after cyber incidents.

NRP 86 will fund interdisciplinary research and includes elements of transdisciplinary research, with practical relevance for owners and operators of critical infrastructures, security practitioners, public authorities, regulators, insurers, researchers and users of critical services. Projects must involve non-academic partners, to contribute to programme-level knowledge exchange, and to produce outputs that can be taken up in policy, governance, organisational practice, technical implementation, training and public decision-making.

The programme has a total budget of CHF 5 million, of which CHF 4.25 million is reserved for research. It is expected to fund approximately five to ten projects across the four research areas. Project budgets must range between CHF 300,000 and CHF 800,000, and research projects may run for 18 to 36 months. Co-financing with other funding sources is explicitly welcomed.

Expressions of interest must be submitted by 24 November 2026, 17:00 Swiss local time, and full proposals by 19 January 2027, 17:00 Swiss local time. Final funding decisions by the SNSF Research Council are expected by August 2027 at the latest. Research under the funded projects must start by 1 November 2027.

2 Introduction

2.1 Background and problem framing

The digitisation of our society offers many advantages but also has associated risks. While the digitisation of critical infrastructures has accelerated, the security of the underlying systems has not kept pace. This critical infrastructure now affects many domains of our lives, including energy supply, healthcare, public and commercial transport, logistics, buildings, communication, agriculture, water supply and sanitation. Switzerland alone has millions of devices connected to the internet – more than the number of residents. Unfortunately, security has not been integrated into most of these connected devices from the beginning, either because threats and vulnerabilities were not known, or because the mitigations are too laborious, complex or expensive for individuals and organisations to implement. Meanwhile, cyberattacks targeting critical infrastructures are increasing, including in Switzerland. Hospitals have been paralysed, ransomware has disrupted public transport, and data breaches have occurred in government administrations. These events highlight the growing fragility of Switzerland's digital fabric. As digitisation is further accelerating, the skills and resources of bad actors are growing ever stronger. There is no end in sight to the increase in the number, variety and scale of attempted attacks.

Like any country, Switzerland has its own challenges and opportunities due to its unique characteristics. The country is small and has a high level of technical development. At the same time, the fragmentation of responsibilities between the Confederation, cantons and municipalities adds to the separation of governing public entities and private operators, complicating coordinated responses. Moreover, like in many other countries, cybersecurity costs are seen as an obstacle to innovation, even though the risk of attacks is widespread.

This NRP is intended to strengthen the resilience of Switzerland's critical infrastructures[1] against cyberattacks. This starts with providing a more solid knowledge base on vulnerabilities and risks with respect to the current digital resilience of the country's critical infrastructures, but also includes identifying technically viable and socially acceptable solutions, as well as proposing comprehensive strategies to put these solutions to work to strengthen the digital resilience of the country's critical infrastructures. Furthermore, it seeks to improve national coordination and governance in the domain of cybersecurity.

2.2 National and international research environment

While Switzerland is highly innovative, it lacks the resources to industrialise ideas. Specialised communities are emerging and collaboration between industry, academia and the government is increasing, but Switzerland still needs stronger legislation, resources and data sharing. Cybersecurity became a national priority in research funding and governmental expertise far earlier in other countries. In Germany, for example, the BSI was established back in 1991, whereas the first steps towards the Swiss NCSC were taken only in 2020. Yet thanks to its political landscape and leading research teams, Switzerland can play a key international role in cyber resilience.

Digital resilience is also an important international issue. For example, the Centre for Cyber Economics (CCE) was created in Saudi Arabia in 2025 by the Global Cybersecurity Forum (GCF) and the World Economic Forum (WEF) as a platform where stakeholders support informed decision-making on cyber resilience. Countries pursue different strategies: the USA and China have shifted towards security policies targeting other countries through regulations and restrictions, while others focus on economics.

[1] For further information on the definition of critical infrastructures in Switzerland, please refer to the Federal Office for Civil Protection (FOCP): https://www.babs.admin.ch/en/critical-infrastructures; additional details are available in the German and French versions of the website.

3 Goals of the National Research Programme

The overarching goal of NRP 86 is to strengthen the resilience of Switzerland's critical infrastructures against cyberattacks in the longer term by investing in developing a state-of-the-art agile collective defence. More precisely, the goal is to improve the ability of the critical infrastructures to withstand, adapt to and recover from digital disruptions, such as cyberattacks or system failures, ensuring operations can continue effectively. This includes improving not only the number and proportion of attacks that critical infrastructures can thwart or resist unscathed, but also the response to successful attacks and their containment (Figure 1).

NRP 86 will improve the resilience of Switzerland's critical infrastructures in sensitive sectors, such as healthcare, transport, agriculture, drinking water and sanitation, by assessing and validating existing defences and developing novel preventive approaches beyond mere technical measures. In order to strengthen the national cyberinfrastructure holistically and in the long run, it is important to further the exchange of relevant information among stakeholders, including government, corporations and academia. Future cybersecurity research needs continuous support through realistic, up-to-date security data. Thus, it is crucial to identify and strengthen coordination and governance mechanisms suited to the fragmented digital landscape. Current processes need to be better understood, assessed and adapted as necessary. These include not only the deployment of defence and protection mechanisms, but also continuous security testing of critical infrastructures and structured responses to incidents. A coherent theory of effective resilience practice is required across fields and types of critical infrastructures. Strategic thinking and established processes are needed to address rising cyberattack rates.

There is still limited understanding of the wider social and economic dynamics that shape cybersecurity and related investment incentives. Strengthening digital resilience in a sustainable and affordable manner requires identifying effective investments and understanding how decisions are made in a context of uncertainty across organisations and interdependent systems, within regulatory and behavioural constraints. As attacks become more sophisticated, relying on insurance to absorb the consequences is increasingly untenable. Security investments can also support business models and generate returns that offset their costs. A collective approach to defence is required, considering all stakeholders and parties, as well as vulnerability to supply-chain attacks and software monoculture. It must be agile enough to adapt swiftly to a rapidly moving landscape, in a global context where nations are increasingly aiming to attain some form of digital self-determination. Moreover, all Western nations now face hybrid warfare, which requires looking at how humans respond to attacks and incidents in order to prepare for attacks that weaponise humans against national infrastructure.

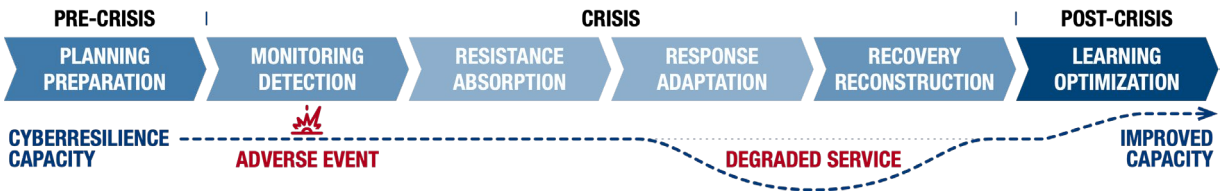

Figure 1: Reaction to a successful attack and implementation of actions to increase digital resilience.[2] NRP 86 aims to avoid successful cyberattacks through a state-of-the-art agile, collective cyber defence and, if attacks occur, to limit their consequences and quickly adapt the strategy in order to prevent future successful attacks.

[2] Adapted from Araujo, M.S.d.; Machado, B.A.S.; Passos, F.U. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Appl. Sci.* **2024**, *14*, 2116. https://doi.org/10.3390/app14052116

4 Main research areas

NRP 86 aims to improve the cyber resilience of critical infrastructures in Switzerland, targeting in particular interdisciplinary and transdisciplinary research activities in the larger ecosystem of cybersecurity. The programme focuses on the four research topics below, which cover not only technical aspects, but also social and human sciences as well as the legal and regulatory framework. Projects are expected to consider both technical and non-technical dimensions in their design in order to meet the programme's interdisciplinary ambition. NRP 86 invites contributions in the following research areas:

4.1 Data

Assessing the current state of cybersecurity, identifying weaknesses and vulnerabilities, conducting research on technical solutions, and coordinating efforts all require data. Academics typically do not have access to data from critical infrastructure providers and thus cannot conduct certain experiments and research or end up overfitting their solutions to singular data points. Governmental institutions have data but cannot simply share it with any interested parties or even among themselves. Similarly, corporations are reluctant to share data for fear of revealing security or business strategies, or of admitting their vulnerabilities. More methodological and usable approaches, and possibly legislation, are required to facilitate and increase the sharing of relevant and actionable data between academia, industry and government agencies. Developing governance frameworks that balance transparency with security requirements and address legal constraints such as data protection obligations under the New Federal Act on Data Protection (nFADP), confidentiality rules while identifying enabling mechanisms, including appropriate legal bases, anonymisation standards and liability arrangements is therefore a priority for this programme.

This research area addresses the conditions – legal, regulatory, contractual and technical – under which *relevant data can be accessed, shared and utilised* for research, operations and public decision-making in Switzerland.

Examples of questions that might be addressed by projects in this research area include:

- *What legal and regulatory frameworks currently enable or constrain data sharing between public authorities, critical infrastructure operators and academic researchers, and how could they be reformed or complemented, including with respect to liability arrangements?*
- *What governance models and institutional arrangements can enable controlled, secure and legally compliant data sharing among stakeholders, including across public and private boundaries?*
- *What are the conditions necessary to allow the sharing of incident and vulnerability data while satisfying data protection requirements? Is anonymisation or pseudonymisation required, and if so, what standards would be sufficient – including in real-time incident response contexts – and how can compliance with these standards be verified in practice?*
- *What mechanisms, including sandboxed research environments and trusted third-party intermediaries, could provide academics with realistic access to operational data without compromising security or confidentiality obligations?*
- *How and under what conditions can data sharing between Swiss federal and cantonal authorities be operationalised, and what legislative or regulatory changes would be required to enable it?*
- *How could international data flows and cross-border incident data affect the legal conditions for data sharing in Switzerland, and how can Swiss frameworks be aligned with EU instruments, such as the Data Act (Regulation 2023/2854) or the NIS2 (Directive 2022/2555), without compromising sovereignty?*

4.2 Best practices

Government institutions and corporations alike often adopt security solutions all too hesitantly, due to perceived barriers to entry or unclear benefits. Processes need to be tested and adapted; while frameworks such as ISO 27001 prescribe ways of doing this, many current best practices in cybersecurity are not tested rigorously. Dealing with supply chain complexity, software monoculture risks and increasing cyberattack rates requires strategic thinking and established processes, including continuous security testing and structured incident response. It is also unclear how practices from one field or type of critical infrastructure may apply to others, and we lack a coherent theory of effective practice for resilience.

This research area addresses *which best practices are state of the art* and how they can be put to work, building a knowledge base that supports the cross-sector transfer of resilience practices and guides future implementation in Switzerland.

Examples of questions that might be addressed by projects in this research area include:

- *What criteria and metrics should be used to assess the effectiveness and return on investment of current practices/solutions?*
- *Which organisational and technical practices currently contribute most to prevention, detection, response, continuity and recovery in Swiss critical infrastructures?*
- *How can successful cybersecurity practices from one sector of critical infrastructure (e.g., energy) be systematically transferred to others (e.g., healthcare or transport)?*
- *How can effective practices for procurement, configuration, patching, monitoring, testing and crisis management be adapted to organisations of different sizes and structures?*
- *What frameworks for supply chain risk management are most effective in reducing exposure to hardware and software risks?*
- *What roles do organisational culture, leadership and communication play in the effective adoption and maintenance of best practices in cybersecurity?*

4.3 Incentives

Many effective solutions for defence and protection are adopted reluctantly due to perceived costs. Corporations view cybersecurity as an expense with no tangible return, sometimes considering the aftermath of attacks less costly based on underestimated probabilities – though the increasing sophistication of attacks challenges such assumptions. Security can support business cases and generate revenues that offset investments. We lack methods to reason about the social and economic system surrounding cybersecurity and the incentives for investment. A better understanding of costs versus benefits and how investment decisions are made despite uncertainty across organisations and interdependent systems is needed for affordable and sustainable resilience.

This research area addresses *what incentives drive investment in security and how they can be increased*, focusing on the economic, regulatory, behavioural and institutional conditions shaping cybersecurity investment decisions.

Examples of questions that might be addressed by projects in this research area include:

- *What economic, behavioural, regulatory and organisational factors jointly explain persistent underinvestment in security in critical infrastructures? How can the value of security and resilience (including financial, operational and systemic benefits, such as the prevention of cascading failures) be quantified and translated into metrics that align with executive decision-making?*

- *How can a 'value of Resilience of Critical Infrastructures' framework be operationalised through decision interfaces (e.g., dashboards, simulations, narratives) and tools to support investment decisions in a context of uncertainty?*
- *What would a practical, adaptive security investment decision tool look like that integrates threat dynamics, organisational risk exposure and sector interdependencies?*
- *What combinations of regulatory and incentive-based mechanisms can align organisational security investments with system-level resilience goals, while accounting for cross-sector interdependencies and avoiding compliance-driven minimalism?*

4.4 Collective defence

Critical national infrastructures (CNIs) are not monolithic systems but rather involve a multitude of hardware and software components, services and the humans that maintain them. Attacks on any constituent element can have ripple effects across larger parts of critical infrastructures, yet providers are commonly unaware of the impacts. Effective resilience therefore requires a form of collective defence that takes all parties into consideration, especially the supply chain. Given that past incidents have weaponised the population, this consideration must extend to end users and beneficiaries of critical services. Starting with awareness of interdependencies, we need research to improve exchange and collaborative risk assessment across parties.

This research area addresses *how we can achieve collective defence across all parties*, focusing on how it can be organised in the Swiss context, how interdependencies can be understood and governed, and how interdisciplinary approaches can bridge technical, organisational, legal and social dimensions across heterogeneous actors in a rapidly evolving threat landscape.

Examples of questions that might be addressed by projects in this research area include:

- *How can interdependencies within and across critical infrastructures be identified, mapped and prioritised for collective risk management?*
- *Which forms of coordination, information exchange and joint decision-making are most effective between operators, suppliers, regulators and response authorities? Which forms of strategic and opportunistic collaboration provide the best starting point for collective defence of CNIs? For instance, can the 'team of teams' model be applied to CNIs?*
- *How can double-loop learning be applied to CNIs? How can lessons from incidents, exercises and near misses be captured and analysed to develop collective defence approaches, formulate more agile responses to intelligence and early warning signals, and improve governance (e.g., distribution of responsibility, developing capability and growing capacity)*?
- *What roles should public authorities, sector regulators and international bodies play in coordinating national cyber defence, and how can these be strengthened in the Swiss context?*
- *What measures can be established to enable and support citizens as an additional layer of defence ('sensors'), such as raising awareness of social engineering and misinformation as attack vectors against critical infrastructures, engaging citizens to provide intelligence or early warning signals, and incentivising access to and sharing of relevant data and the verification of its validity (using AI or mutual verification, community activities, etc.)?*

5 Implementation and expected outcomes

5.1 Implementation

The following implementation pathways may be pursued to achieve the expected outcomes:

- Strengthening interaction among stakeholders through project-led research, programme-level outreach, partnerships with existing initiatives and cross-sector exercises.
- Establishing data-sharing channels and related legal and governance frameworks (covering data protection provisions, anonymisation standards, permitted uses, confidentiality obligations and liability rules), treating these as expected programme outputs rather than assumed preconditions.
- Supporting the implementation of cyber resilience workflows, guidelines, protocols and methods for continuous testing, incident response, recovery and adaptation, supplemented by official policies and regulations where needed.
- Producing a range of outputs, including practice-oriented publications, teaching and training materials, peer-reviewed scientific publications, FAIR datasets, validated tools and public communications across multiple media; creating pilot-tested products or solutions where applicable.
- Actively engaging academic project teams in professional and non-academic venues to foster data-sharing dialogue and meaningful interactions with practitioners.
- Encouraging direct involvement of stakeholders in research projects through practice partnerships and co-funding arrangements that address incentives, supply-chain and monoculture risks, and human factors.
- Designing outreach and partnership-building activities alongside legal frameworks that provide adequate protection to participating stakeholders through confidentiality safeguards and clear governance rules on how shared information may be used by research teams and public authorities.

5.2 Expected outcomes

NRP 86 aims to strengthen digital resilience in Switzerland by producing practice-oriented knowledge, validated tools, governance models and coordination mechanisms for critical infrastructures.
Its potential outcomes include the following:

- Implementation of a state-of-the-art agile collective cyber defence and development of a theory of effective practice with post-incident learning for resilience.
- Enhanced communication and collaboration between academia, practitioners and other stakeholders, with research solutions actively taken up by non-academic actors, particularly critical infrastructure owners and operators.
- Increased sharing and exchange of relevant operational, incident and vulnerability data between parties, e.g., academic researchers, critical infrastructure operators and government agencies.
- Progress in the implementation and adoption of guidelines, regulations, protocols and policies for testing defences, prioritising investments and coordinated responses to strengthen cyber resilience.
- Attitudinal and behavioural changes among owners, operators and end users of critical infrastructures, leading to greater preparedness for social engineering, misinformation and hybrid threats.
- Training of a new generation of leaders in digital transformation with broad expertise in cyber resilience, extending beyond purely technical knowledge.

6 Characteristics of the NRP and requirements for research

6.1 Solution-oriented focus

All projects are to be oriented towards research areas 1, 2, 3 or 4, and ideally more than one of these. Moreover, projects must be solution-oriented and relevant to practice. Project proposals should include a discussion of the project's practical relevance and concrete proposals for the practical implementation of the project results. NRP 86 will not fund basic research that does not generate any practice-oriented outcomes. Applicants should propose outreach activities to foster interactions with stakeholders.

6.2 Interdisciplinary research approach

Cybersecurity is a multifaceted problem involving many stakeholders, as outlined above. The success of the proposed programme critically depends on the close cooperation of specialists from different disciplines, including but not limited to representatives from the following fields:

- Cybersecurity (data/information security, system security, software security, applied cryptography)
- Behavioural science (trustworthiness, usable security, security education/training)
- Law, regulation and public policy (data protection and privacy, liability regime, contract law, regulatory design and public law governing critical infrastructure)
- Socioeconomics (incentives, supply chain)

Therefore, **all projects must substantively address both technical and non-technical dimensions of digital resilience**, including, where relevant, human, legal and organisational aspects. Applicants will be required to describe this integration explicitly in a dedicated section of the proposal.

6.3 Elements of transdisciplinary research

Because the programme seeks to generate knowledge and solutions that are relevant, applicable and grounded in the realities of Switzerland's critical infrastructures, **all projects are required to include at least one non-academic partner**. This partner must operate within, provide services to, regulate, support or be otherwise directly involved in a sector or function relevant to critical infrastructure. This may include operators, service providers, public authorities, regulators or other stakeholders whose work affects the resilience, continuity or security of critical infrastructure services.

The success of NRP 86 will depend on timely knowledge exchange, concrete stakeholder involvement and the translation of research outputs into usable practices. Applicants are expected to specify when and how the non-academic partner(s) will be involved over the course of the project, so that this involvement is concrete, timely and meaningful rather than merely formal. The main stakeholder groups considered in NRP 86 are summarised in the following table:

Stakeholder group	Role in NRP 86
Critical infrastructure owners	Decision-makers accountable for resilience strategy, resources and governance
Operators and technical staff	Run services, maintain systems, handle incidents and provide operational knowledge and data
Security practitioners and experts	Assess threats, design and test defences, translate research into operational security practice
Critical-service staff and users	Use critical systems to provide services and help evaluate usability, workflows and adoption
Clients, customers and citizens	Depend on critical services and may be affected by outages, misinformation, social engineering, etc.

Insurers	Price and transfer cyber risk, influence disclosure practices, and help shape investment incentives
Legal officers, legislators and regulators	Define legal bases, confidentiality rules, liability models, regulatory instruments, policy conditions
Policy makers and public authorities	Use findings for public decisions, coordination mandates, crisis preparation and resilience agendas
Security researchers and academic partners	Generate evidence, methods, frameworks, tools, FAIR datasets and cross-disciplinary training

Research plans must include a convincing implementation strategy: Applicants are asked to define clearly formulated and implementable project outcomes that can realistically be taken up in practice, policy, governance, organisational processes or technical implementation.

6.4 Data access, data management and open research data

The outcomes of publicly funded research should, as far as possible, be accessible to the public free of charge. The SNSF is committed to this goal through Open Science (snf.ch). For most funding schemes, researchers must include a data management plan (DMP) in their application. At the same time, the SNSF expects data generated by SNSF-funded projects to be publicly accessible in FAIR digital databases (ensuring that data are Findable, Accessible, Interoperable and Reusable), provided that there are no legal, ethical, copyright or other problems.

7 Submission and evaluation procedure

7.1 General conditions

Legal basis: Proposals must be in line with the regulations outlined in this call document. In addition, and if no specific provision is formulated in this call, the SNSF Funding Regulations and the General Implementation Regulations for the Funding Regulations apply. Only one call for proposals is envisaged; however, in the event of significant thematic gaps, a second call may be launched.

Coordinated research and programme activities: National Research Programmes contribute towards solving pressing challenges of national significance. To this end, the Steering Committee coordinates and manages the selection of projects, the research carried out and other NRP-specific activities, such as regular programme meetings and stakeholder exchange. The Steering Committee will maintain continuous contact with key stakeholders throughout the programme and will ensure their participation in activities carried out within its framework. The aim is to ensure the quality of the research, enable synergies and disseminate the projects' outcomes to relevant target audiences. By submitting a project proposal to NRP 86, applicants agree to participate in the programme activities, cooperate with the Steering Committee and the programme management, and contribute to the collective results of the programme.

Project start: Approved research projects must begin no later than 1 November 2027.

Project duration: Research projects conducted under NRP 86 must run for a minimum of **18** months and a maximum of **36** months.

Project budget: The grant requested for a project must amount to at least **CHF 300,000** and may not exceed **CHF 800,000**, irrespective of the number of researchers involved or the duration of the project. Additional financing from other funding sources (*e.g.* from non-academic project partners) is explicitly

welcomed (Article 18 of the SNSF Funding Regulations and Chapter I, paragraph 1.20 of the General Implementation Regulations for the Funding Regulations).

Salaries: The salaries of applicants will not be funded by NRP 86. Applicants intending to employ PhD students with NRP 86 project funds must ensure appropriate funding for the remaining duration of their doctoral studies, including any period extending beyond the end of the NRP 86-funded project. They must also demonstrate how the doctoral work will contribute to the project and how relevant dissertation results will be incorporated into the final report.

Language of proposals: Expressions of interest and full proposals must be submitted in English.

7.2 Eligibility criteria for applicants and project partners

Applicants: Applicants are required to fulfil the requirements of Article 10 of the SNSF Funding Regulations. Applicants with a doctorate must have obtained the latter no less than four years before the submission date of the application. Applicants without a doctoral degree must demonstrate at least three years of full-time research activity.

An applicant must be in a position to be fully responsible for carrying out a research project and managing the staff involved in it. Conflicts of interest and incompatibilities are assessed in accordance with the SNSF regulations on recusal and conflicts of interest. Applicants who are family members, are in a personal relationship with each other or may otherwise be perceived as lacking independence cannot collaborate scientifically on the same project, particularly where hierarchical relationships are involved.

Number of projects: Each applicant may submit only one proposal under this call and may not participate as a project partner in any other proposal of this NRP. Non-academic project partners may participate in more than one proposal. A proposal may be submitted regardless of the number of other SNSF grants held or applied for, provided that the regulations of the relevant funding instruments are complied with.

During the evaluation process, applicants may not have identical or substantially similar proposals under evaluation in another SNSF funding scheme with overlapping funding periods (cf. Article 17 of the SNSF Funding Regulations).

Eligibility of project partners: Project partners are researchers and/or non-academic actors who make a partial contribution to the research project without being responsible for the project. They are eligible according to the SNSF Funding Regulations and the General Implementation Regulations for the Funding Regulations. Applicants who wish to conduct the planned research in collaboration with a commercially oriented institution must be able to prove to the SNSF that the principles of research freedom, research independence and freedom to publish will be upheld. As with the applicants, project partners' own salaries will not be funded by NRP 86, and the share of the total budget allocated to project partners should generally not exceed 20%. Project partners must not refer to the support received from the SNSF as a grant they have themselves acquired.

Cross-border research projects: Collaboration with research groups in other countries is allowed, provided that such cooperation either generates significant added value **that could not be achieved without cross-border cooperation** or substantially enhances the proposed research with respect to content or methodology, or if the competencies of researchers from abroad are essential for the successful completion of the project. As a rule, the funding share requested for co-applicant researchers

abroad may amount to 30% of the requested research budget. For co-applicants from abroad, the norms and salary rates of the relevant country will be applied mutatis mutandis, with the SNSF maximum rates as the upper limit. Before submitting a proposal with a cross-border component, please contact the programme manager for NRP 86.

7.3 Submission procedure

The application procedure for this NRP consists of a two-step process, with an initial submission of an expression of interest (not reviewed) and subsequent submission of a full proposal, which will undergo international peer review. Please note that all applicants and project partners must enter their personal data, including CV, in the SNSF portal **themselves**. Only then can you submit your expression of interest. Invite all applicants and project partners as contributors to the proposal **early on**, so that they have enough time to create a user account if necessary and to enter their data in the portal. **Once the submission deadline for the expression of interest has passed, it will no longer be possible to apply to this NRP.**

7.3.1 Online submission via the SNSF Portal

To submit a proposal via the SNSF Portal, applicants and project partners must log in with a SWITCH edu-ID. Step-by-step instructions are provided for the initial login (Create an SNSF Portal user account).

CV: Applicants must compile their CV according to the template on the SNSF Portal.
Information can be found on the CV website and on the SNSF Portal.

7.3.2 Expression of interest

The template for full proposals is provided on the SNSF Portal and on the website nfp86.ch at the expression of interest stage.
Applicants must submit an expression of interest, including personal data, team composition and an abstract of the proposed project (4,000 characters max.) via the SNSF Portal by **24 November 2026**, 17:00 Swiss local time. Project partners confirm their participation by entering their administrative data on the SNSF Portal. The expression of interest and the provided information allow the SNSF to organise the upcoming evaluation process. There will be no evaluation or pre-selection at this stage.

The expression of interest will be accepted on 25 November, and applicants will then be able to complete the full proposal on the portal.

7.3.3 Full proposals

The deadline for submitting full proposals is 19 January 2027, 17:00 Swiss local time.

Full proposals must be submitted online via the SNSF Portal. In addition to the administrative data to be entered directly in the SNSF Portal, the following documents need to be uploaded:

- **Project plan and bibliography** (in PDF format): Applicants must use the template provided in the SNSF Portal. The project plan must not exceed 15 pages (excluding bibliography).

Please note that formal letters of support from non-academic project partners must be submitted at a later stage.

7.4 Project selection procedure

The SNSF office checks whether the personal and formal requirements are met before forwarding the proposal for scientific review. The SNSF will not consider proposals that do not meet the personal and formal requirements. The applicants will be notified of such a decision by means of a formally appealable ruling.

The Steering Committee may carry out a preliminary evaluation of proposals and exclude from further consideration those that fall outside the objectives and scope of NRP 86. The SNSF shall notify the applicants of such a decision in the form of an appealable ruling.

The full proposals selected to proceed to the next stage are evaluated by national and international experts. Based on these external reviews and the evaluation criteria set out below, the Steering Committee assesses the full proposals and formulates a funding recommendation. During the evaluation phase only, ad hoc experts may be appointed to provide specific expertise and complement the evaluation panel alongside the Steering Committee. In formulating its recommendation, the Steering Committee takes into account the overall coherence of the selected projects with the programme's objectives, as well as the transparent and consistent application of the evaluation criteria. Final funding decisions are taken independently by the National Research Council.

7.5 Evaluation criteria

Eligible full proposals are evaluated based on the following criteria:

- **Compliance with the goals of NRP 86 and relevance to its research questions:** Full proposals must correspond to the programme goals specified in this call for proposals and fall within the overall framework of the programme;

- **Scientific quality of the research project:** Scientific relevance, topicality and originality, suitable methods and feasibility;

- **Interdisciplinary integration:** Coherence and added value of the combined technical and non-technical disciplinary knowledge, including, where relevant, human, legal and organisational aspects, to address complex interdependencies and systemic risks;

- **Practical relevance:** Credibility of a structured implementation strategy involving relevant stakeholders and non-academic actors, with clear responsibilities and timelines, and strong steps to achieve actionable results for governance or practice;

- **Scientific qualifications of the applicant(s) and suitable infrastructure:** Scientific track record in the field of the proposal and ability to carry out the research project.
  Adequate personnel resources and a suitable infrastructure must be secured.

8 Programme budget and schedule

8.1 Programme budget

It is expected that NRP 86 will fund approximately five to ten projects across all four research areas.

Projects	Research area 1: Data	CHF 4,250,000
	Research area 2: Best practices	
	Research area 3: Incentives	
	Research area 4: Collective defence	
Knowledge exchange and synthesis		CHF 300,000
Cross-project and programme-level coordination		CHF 150,000
Scientific evaluation, support and steering		CHF 300,000
Total budget		**CHF 5 million**

8.2 Schedule

The individual projects of NRP 86 can have a maximum duration of 36 months.

Publication of the call for proposals	22 September 2026
Deadline for submission of expression of interest	24 November 2026
Deadline for submission of full proposals	19 January 2027
Final decision on full proposals by SNSF Research Council	no later than August 2027
Start of research	no later than 1 November 2027
End of research	November 2031
Publication of the programme synthesis	Mid 2032

9 Organisation and actors

Steering Committee of NRP 86

- Professor Pascal Felber, Professor of Computer Science,
  Department of Computer Science, University of Neuchâtel (President)
- Dr Eva Cellina, Admitted to the Swiss bar and Lecturer,
  Digital Law Center, Faculty of Law, University of Geneva
- Dr Fabian Muhly, Deputy Head in Defence Economics/Cyber Defence,
  Military Academy at ETH Zurich
- Professor Martina Angela Sasse, Professor of Human-Centred Security,
  Horst-Görtz-Institut für IT-Sicherheit, Ruhr-Universität Bochum (Germany)

Representative of the Swiss Federal Administration

- Dr Bernhard Tellenbach, Head of Cyberdefence,
  armasuisse Science + Technology

Delegate of the Research Council Thematic and Solution-oriented Research (TSOR)

- Professor Patrick Eugster, Professor of Computer Science,
  Computer Systems Institute, Università della Svizzera italiana

Programme Manager

- Dr Martin Christen, Swiss National Science Foundation, Berne

Programme Assistant

- Julien Jauquier, Swiss National Science Foundation, Berne

10 Contacts

For questions regarding the submission of expressions of interest and full proposals, please contact Martin Christen, Programme Manager: nrp86@snf.ch or +41 31 308 22 22.

For questions concerning salaries and eligible costs, please contact Roman Sollberger, Head of Finance: roman.sollberger@snf.ch or +41 31 308 22 22.

For technical help with the SNSF Portal and electronic submissions, please access the SNSF Support Portal: https://snsf-ch.atlassian.net/servicedesk

Hotline: tel. +41 31 308 22 00 (Deutsch/Français/English)